ISSN (ONLINE):2045-8711
ISSN (PRINT):2045-869X

International Journal of Innovative Technology and Creative Engineering

August 2024
Vol-14 No:-8
@ IJITCE Publication

UK: Managing Editor
International Journal of Innovative Technology and Creative Engineering
1a park lane,
Cranford
London
TW59WA
UK

USA: Editor
International Journal of Innovative Technology and Creative Engineering
Dr. Arumugam
Department of Chemistry
University of Georgia
GA-30602, USA.

India: Editor
International Journal of Innovative Technology & Creative Engineering
36/4 12th Avenue,
1st cross St,
VaigaiColony
Ashok Nagar
Chennai, India 600083

Email: editor@ijitce.co.uk

www.ijitce.co.uk

IJITCE PUBLICATION

International Journal of Innovative Technology & Creative Engineering

Vol.14 No.08

August 2024

IJITCE
INNOVATE TO CREATE

www.ijitce.co.uk

Dear Researcher,

Greetings!

Articles in this issue discusses about recent trends in smart card technology.

We look forward many newer technologies in the next month.

Thanks,
Editorial Team
IJITCE

Editorial Members

Review Board Members

Contents

SECURITY ANALYSIS OF ELECTRONIC VOTING SCHEME USING SMART CARD TECHNOLOGY

Dr. V.K. NARENDIRA KUMAR
Assistant Professor, PG & Research Department of Computer Science,
Gobi Arts & Science College (Autonomous),
Gobichettipalayam – 638 453, Erode District, Tamil Nadu, India.
Dr. V.K. MANAVALASUNDARAM
Professor, Department of Information Technology,
Velalar College of Engineering and Technology, Erode, Tamil Nadu, India.

Abstract- Voting is regarded as one of the most effective methods for individuals to express their opinions to select their democratic leader in the public elections. As the computing, communicating, and cryptographic techniques progress rapidly, increasing emphasis has been placed on developing electronic voting schemes capable of providing more efficient voting services than conventional paper-based voting methods. It has been widely recognized as a secure electronic voting scheme, which satisfies not only completeness, privacy, unfeasibility, eligibility, fairness, verifiability, and robustness, but also receipt-fairness. A receipt-free e-voting scheme based on the virtual voting booth that can be implemented with a smart card. Receipt-freeness is achieved by distributing the voting procedure between the voter and the smart card. The voter and the smart card jointly contribute randomness for the encryption of the ballot. To provide convenience to voters, sufficient voting facilities are supplied in sufficient public voting booths. Unlike conventional paper-based voting systems the voter can choose any voting booth that is convenient and safe to them in the proposed e-voting scheme. By using smart cards to randomize part of content of the ballot, the voter cannot construct a receipt

Keywords: Smart Card, Election, Internet, Voting, Digital Signature, Public Key, Identification, Registration & Security.

1. INTRODUCTION

Elections are one of the most critical functions of the democracy. Not only do they provide for the orderly transfer of power, but they also cement citizen's trust and confidence in government when they operate as expected. Internet systems are among those being considered to replace older, less reliable systems. Election systems, however, must meet standards with regard to security, secrecy, equity, and many other criteria, making internet voting much more challenging than most electronic commerce or electronic government applications [1].

1.1. Internet Voting by Type

Internet voting systems can be grouped into three general categories: poll site, kiosk, and remote. Each of these categories define the location where the ballot is cast, which, in turn, defines the social science and technical hurdles that are associated with each type of system. Poll site internet voting offers the promise of greater convenience and efficiency than traditional voting systems in that voters could eventually cast their ballots from many polling places and the tallying process would be both fast and certain. Remote internet voting seeks to maximize the convenience and access of the voters by enabling them to cast ballots from virtually any location that is internet accessible. While the concept of voting from the home or work is attractive and offers significant benefits, it also provides substantial security risks and other concerns relative to civic culture. Without official control of the voting platform and physical environment, there are many possible ways for people to intervene to affect the voting process and the election results [8].

1.2. Conventional Voting Systems

Paper Ballots: Voters mark boxes next to the names of candidates or issue choices, and place them in a ballot box. The ballots are counted manually. Paper ballots are also widely used for absentee ballots. Their drawback is that counting is laborious and subject to human error.

Mechanical Lever Machines: Voters cast ballots by pulling down levers that correspond to each candidate or issue choice. Each lever has a mechanical counter that record the number of votes for that position.

The machines prevent voting for more than one candidate. These machines are still widely used, but are no longer manufactured. Some versions do not produce an audit trail.

Punch Cards: Voters punch holes in computer readable ballot cards. Some systems use mechanical hole-punch devices for punching the holes while others provide the voter with pins to punch out the holes. The latter have been more subject to incomplete punches, resulting in more errors in reading the cards.

Optical Scan Devices: Voters record choices by filling in a rectangle, circle, or oval on the ballot. The ballots are read by running them through a computer scanner, which then records the vote [2].

Direct Recording Electronic (DRE) Devices: Special-purpose or PC-based computers are used as voting machines. Voters use touch screens or push buttons to select choices, which are stored electronically in the memory of the machine. There are no paper ballots and no paper record independent of the electronic memory.

1.3. Criteria for Election Systems

Voting Principles: In general, the requirements for conventional, “paper based” voting also apply to electronic voting. These principals for democratic elections can be expected to be universal; of course, voting procedures may differ in many details.

Free Elections: The citizen must be able to use their voting rights without being coerced and without undue influence of a third party.

Secret Voting: No person must know the vote of another person.

Equal Voting Rights: Each vote must have the same weight. No vote must become invalid by predictable technical problems or must be lost on its way to the voting authority. Also, the right to vote must not be made dependent on factors other than those enumerated in the Law.

Audibility: The whole voting process must be transparent and reproducible.

Flexibility: The system should be configurable for many different election scenarios like different ballot question formats or multiple languages act and on a technical level compatible with multiple operation system platforms as well.

Uniqueness: No voter should be able to vote more than once.

Convenience: Election systems should not require extra skills to be usable and without unreasonable need for equipment [10].

1.4. Traditional Paper Based Voting

The electronic voting systems are based on the traditional paper based voting. Paper based voting is composed by a voting authority and the voters who are willing to express their whishes through the vote. The voting process as follows:

- The voter is registered to vote by the voting authority. Usually a paper based identity is issued in the name of the voter.
- In the day of the election, the voter’s proceeds to the designated voting section, where it presents its voting identity.
- The voting authority representative verifies the identity of the voter and gives permission for the voter to cast the vote. A paper with the voting options is given to the voter.
- The voter proceeds to the secret ballots, where the voter writes in the official voting paper the whishes. The vote is cast into a sealed ballot.
- After all votes are cast, the voting authority gathers all ballots and counts all votes. If a recount is necessary, the same ballots are recounted.

1.5. Electronic Voting Systems

An electronic voting system is an evolution of the paper based voting system. It comprises several forms of electronic devices such as electronic voting machines in kiosks, voting via internet, punch machine ballots with optical scanners, voting via email, etc. The same principles that are valid for the paper based voting are also valid for the electronic voting process.

2. LITERATURE SURVEY

Electronic voting schemes without any security are unsuitable for being deployed in large-scale environments because a failure of a single voter would disrupt the entire voting. An electronic voting scheme based on the sender untraceable email system, which assumes that at least one mix is trust. Based on multiple key ciphers, a voting scheme, in which the voting authority can easily falsify the ballots. The security of their electronic voting schemes relies on the cooperation of the voters.

Proposed voting scheme is based on the homomorphic encryption technique, which can conceal the content of ballots, in a homomorphic encrypted ballot through the public channel, which is often implemented by a bulletin board. The encrypted ballots can be decrypted by any set of at least authorities. In the proposed a receipt-free and uncoercible electronic voting scheme is implemented with a smart card. The voter and the smart card jointly contribute randomness to the encryption of the ballot. Within the virtual voting booth, the voter interactively communicates with his smart card.

2.1. Electronic Voting using Smart Card

In electronic voting systems the ballot box is remote and the voter uses computer networks to deliver the vote [5]. This voting system provides the voters with many benefits, such as the ability of issuing the vote from many different voting points and the possibility of getting the election result quickly.

As elements of the general system architecture, smart cards have two essential functions:

a. To guarantee the authentication of the voter. Based in a set of keys and personal data stored in the cards, the voter is able to demonstrate their right to participate in the election. Similarly, the different management authorities and supervisors of the system have their own smart cards to guarantee the proper authentication.

b. To be a reliable device to carry out certain cryptographic operations. Smart cards that are able to execute public key algorithms strongly guarantee the security the security of the operations and the privacy of the voters, facilitating the anonymity of the chosen option [7].

3. PROCESS REQUIREMENTS DURING VOTING

The average citizen cannot understand their internal requirements. Given that the people have a constitutional “right to designate the rulers of the state” it is not able that ownership and scrutiny of the casting, collecting and counting of votes has become a secret matter. In response to this, concerned private citizens have made use of the Freedom of Information to obtain as much relevant information as possible. People are getting more used to work with computers to do all sort of things to vote far from where they usually live, helping to reduce abstention rates. They may support arbitrary voting ballots and check their correct fulfillment during the voting process.

Authorization for Internet Ballot: The authorization for Internet balloting can be in various forms depending on the design of the Internet voting system as a whole. But any authorization must provide a way of linking the eventual vote cast using that registration to the registration record for that voter. So that it can be determined beyond a reasonable doubt that each Internet vote is associated with a registered voter in the proper district, and that at most one vote is counted for any voter. A server’s response to the request for an Internet ballot will normally be to issue an authorization for Internet balloting to the voter who requested it. The authorization will be some combination of cryptographic keys, or PINs, or both, possibly accompanied by voting software.

Loss of Internet Ballot Authorization: Any system must be able to handle the voter’s loss of, or failure to use, authorization for Internet balloting. If a voter loses Internet ballot authorization, or if that authorization for some reason fails to work to allow voting, then the voter can request a new Internet authorization. Before either such request is granted, the old authorization must be cancelled.

Voter Authenticates Their Self: Voters should be provided with an authentication code from the server that is combined with a Personal Identification Number (PIN) that will allow the voter to authenticate him/herself for the Internet voting system.

Voter Brings Internet Ballot to Screen: The screen on which the user views the ballot must be capable of rendering an image of the ballot in any of the languages and orthographies required by law for paper ballots. The application used for voting should not display or play any advertisement. Multi-page ballots should be easily navigable by voters, with no way to get lost or leave the balloting process except deliberately.

Voter makes choices: Voters should be able to point and click to make their voting selections. They should be able to navigate back and forth within the ballot to change selections freely until the moment when they click the final button that irrevocably transmits their ballot. Needs of voters with disabilities or impairments should be accommodated. The actual contents of the voter’s votes on the client computer should be kept only in volatile memory.

Voter Casts Ballot: No vote must be transmitted before the voter clicks on a next-to-final button labeled, "Send Ballot". After clicking, the voter must be told that sending the ballot is final and must be asked to confirm voter intention to send the ballot by clicking a "Confirm" button. If the voter does not click the "Confirm" button, they should be able to return to the ballot to continue voting [5].

Ballot Transmitted to Vote Server: The ballot, along with a timestamp, voter's identification, precinct, and any other appropriate information, must be transmitted to the vote server in encrypted form to protect the privacy and integrity of the information.

Vote Server Receives Ballot: The ballot transaction is atomic. A ballot must be either wholly accepted, or wholly not accepted, by the vote server. There must be no middle ground. The vote server that receives a ballot should immediately check it to ensure that it is formatted correctly. If it is, the vote server should immediately store the ballot, still encrypted, on a permanent medium. So that any subsequent power or equipment failure will not lose the ballot.

Vote Server Sends Feedback to Voter's Screen: Within a few seconds of receiving the ballot, the vote server should attempt to notify the voter of whether or not the vote was successfully accepted. If no feedback comes back to the voter's computer within a reasonable time, for any reason, then the voter is entitled to assume that the vote was not accepted, and may try again to vote.

Voter Can Ask For Confirmation after Casting of Vote: There must be a mechanism that voters can use to determine the status of their vote, whether or not it has been accepted and authenticated. After the voter has sent the ballot to the vote server, there must be no way for anyone, even the voter, to determine how they voted in any contest. In particular, there must be no way that a voter can prove to a third party how voter voted [6].

Votes Transmitted from Vote Server to Canvassing Machines: Internet voting systems must be capable of accurately tabulating the results and integrating the results with the server's primary voting system.

Authentication of votes and separation from voter identification: The election system server must be able to verify the authenticity of a ballot before the votes on the ballot are viewed or counted.

Canvassing of Votes: The Internet voting system must be capable of accurately tabulating the results of all ballots cast. The canvass should only be conducted after the close of polls on Election Day.

Maintenance of Auditing Information: Decrypted ballots must retain in a secure format to allow for subsequent auditing and recount procedures [11].

4. IDENTIFICATION SYSTEM

The system can be grouped in 3 different classes: PIN-Based or TAN-Based systems using smart cards for identification.

4.1. Pin-Based Systems

The voter is an identification user on the internet, after login the ballot sheet can be filled out and sent in, where the communication between the browser and the voting server is secured using cryptographic standards; it is obvious that anonymity cannot be guaranteed. Such systems can lower the transaction costs for elections drastically and in the case of dislocated voters be prerequisite for a fast election.

4.2. TAN-Based Systems

Number are issued and the election in usually possible by using the TAN in a Web browser. The connection between the voter and the Web server is also secured is also secured and the cryptographic key is issued by a Trust Center. The voter receives a random number as a receipt for casting the vote, which can be used to check whether the vote entered the tally correctly at a different Website.

4.3. Smart Card-Based Systems

Hence, neither PIN nor TAN based systems can be used for democratic elections, however, both are relatively easy to implement and can be used or a wide range of voting applications, where requirements for anonymity are less stringent or where anonymity is not a requirement at all. Systems using smart cards for digital signatures, which also enables the use of cryptographic methods is the choice for electronic voting [6].

4.4. One-Stage Smart Card-Based Systems

The algorithm assumes the use of a trust center for obtaining each party's public signature or crypto key. In its basic layout, the algorithm follows the registration – ballot box approach. The voter first authenticates the registration's digital signature $S^{R}_{prtv\ at}$ the latter's Trust Center and then removes the blinding layer from the signature obtaining σ(m (BS)). The voter obtains a pair of m (BS), σ(m (BS)) authenticated by the registration.

This algorithm has been implemented in various variations but all variants still maintained the basic problem: it is a one-phased algorithm, which means that both steps, identification and voting, are completed in one stage. When the administration of the registration and ballot box servers collude, it is possible to break the anonymity as well as to vote for voters that were entitled to vote but did not do so. The algorithm is secure on the application level, however, if the browser-based application provided by the registration step fraudulently stores the IP address for each blindly signed ballot sheet, and passes on this information to the ballot box, the m(BS) – and eventually also the clear-text ballot sheet after submission of m' can be linked to a voter later. Also temporary files could be used for this purpose. Hence, anonymity cannot be guaranteed if registration and vote submission are processed in one stage [9].

4.5. Two-Stage Protocol

The proposed algorithm strictly separates registration and vote submission stage.

Registration Phase: The voter's credentials are checked and the voter receives a blindly signed election token, which is securely stored.

Voting Phase: The voter uses the election token to obtain a ballot sheet and casts her vote.

5. STORAGE MEDIA

As the algorithm uses a two-phase-protocol there is the need to temporarily store the token on a secure, anonymous medium.

On the smart card used for the digital signature

The advantage of storing the token on the voter's smart card is the protection from data loss as compared to conventional storage media and the protection from unauthorized access when the token is secured by a PIN from read in.

The source code of the e-voting software can be made generally available and can be submitted to certification by an independent authority showing that neither the personal data nor the card number is accessed by the voting software, however, it seems doubtful whether this will be sufficient to gain public acceptance and since election token resides on the card between registration and election day, any other application accessing the card may read the personal information plus the token stored on the card thereby enabling a third party to trace the vote later [4].

On any storage medium similar to an electronic purse

This variant solves the problems with serial number and clear text information discussed above: the voter uses a floppy disk or an USB-memory-key during the registration process and the token is saved on it. The implementation would be easy and would rely on general purpose infrastructure which is available off shelve.

On a smart card other than the smart card used for digital signature

Another possibility would also be the use of a processor smart card, whose serial number is not registered or a storage card with in a minimum of processor functionality pure storage cards can be read and written to by general purpose card readers and in both variations there is no need for additional hardware. In both case, the card used for the digital signature is used only for identification purposes during the registration phase only and the token is stored on the second card. During the voting phase, only the storage card is used and anonymity can be preserved [3].

6. IMPLEMENTATION OF INTERNET VOTING

Implementation is the process of converting a new system design into operation. Implementation is the key stage in achieving a successful new system as it involves a lot of upheaval in the system development process. This is carefully planned and controlled. A Primary implementation plan is prepared to schedule and manage many different activities that must be completed for a successful system implantation. The primary plan serves as a basis for checking the availability of resources for implementation activities.

6.1 Steps for Various Phases

Voting systems usually lead to a biased result that imparts the desired democracy. Unfortunately, these two problems become more difficult to solve when using e-voting schemes. Although many e-voting schemes have been proposed to provide receipt-freeness to solve these problems, none is both secure and practical. In this research, an e-voting scheme that can solve or at least lessen the problems of bribe and coercion can be realized with current techniques. The techniques used for various phases are given below:

6.1.1 Ballot Generation Phase

Step G1: Voter i goes to a VB that is convenient and safe for him, and authenticates himself to VB with his smart card SC_i, that has been activated by his biometric characteristic.

Step G2: Voter i uses SC_i to generate random numbers r_j (j = 1…L), and then uses SC_i to compute e(j) = (g^{rj}, h^{rj} G_j) (j = 1...L). Next, Voter *i* sends {e(j)| j = 1…L} to VB.

Step G3: VB generates random numbers R_j (j= 1…L) and computes E(j) = (e_1(j) g^{Rj}, e_2 (j) h^{Rj}) (j = 1...L), where e(*x*) = (e_1 (*x*), e_2 (*x*)). VB generates random numbers D_j (j= 1…L), and computes (a_j, b_j) = (g^{Dj}, h^{Dj}) (j = 1…L), Next, VB generates random numbers w_j and N_j (j= 1…L), and computes $s_j = g^{wj}$ h^{RjNj} (j= 1…L). Then, VB sends {E(j), (a_j, b_j) s_j | j = 1…L} to Voter *i.*

6.1.2 Ballot Casting Phase

Step C1: Voter i uses SC_i to generate random numbers, d_j, k_j and w_j´, and compute a_j, = $(x_j)^{dj}$ g^{kj} (j = 1…., z – 1, z + 1, …., L), $b_j = (y_j)^{dj}$ h^{kj} (j = 1…., z – 1, z + 1, …., L), $a_z = g^{w_z + w_z'}$, and $b_z = h^{w_z + w_z'}$, where z □, (1,2,..., L,} is the number representing the option selected by Voter i. Then, Voter i uses SC_i to compute B = H (ID_i x, y x_1, …, x_L, y_1…y_L, a_1..., a_L, b_1, …, b_L) and d_t = B, d_j (j = 1…L).

Step C2: Voter i sends {B, d_j| j= 1.L} to VB.

Step C3: VB sends {$k_J = w_j + R_j$ d_j | j = 1…L} to Voter i.

Step C4: Voter i uses SC_i to compute $R_z = w_z' - k_z$ $d_z + K_z$, Voter i sends {E (z) B, d_1, d_z, …, d_L, r_1, r_2…, r_L with signature} to BB.

6.1.3 Step for Tallying Phase

Voting Authorities compute (X, Y) = (!Cx_i, ! Cy_i), where x_i and y_i denote the valid x and y of Voter i, respectively. Next, Voting Authorities jointly (atleast t voting authorities) compute $W=\frac{Y}{X^s} = G_1^{T_1} G_2^{T_2} ... G_L^{T_L}$. Then, Voting Authorities determine final tally T_1, T_2, …., T_L from W, and announce the Result.

The system is developed using J2EE standards, implementation is much easier compared to other technologies. For implementation, there is a need for application server like Internet Explorer 6.0(or Higher Version). In the application server all the class files like jsp, HTML files will be placed in application folder.

7. EXPERIMENTAL RESULTS

Poll site Internet voting systems offer some benefits and could be responsibly fielded within the next several election cycles. While many issues remain to be addressed, the problems associated with these systems appear likely to be resolvable in the short term. As such, it is appropriate for experiments to be conducted and prototypes deployed in order to gain valuable experience prior to full-scale implementation. This would provide a basis for evaluating poll site voting compared to other voting systems. For instance, voters might first cast their ballots at the precinct level, then from anywhere within the county, and finally from anywhere within the state. The later step would require registration and voter systems in the different counties to work together.

Remote Internet voting systems pose significant risk to the integrity of the voting process, and should not be fielded for use in public elections until substantial technical and social science issues are addressed. The security risks associated with these systems are both numerous and pervasive, and in many cases cannot be resolved using even the most sophisticated technology today. In addition, many of the social science concerns regarding the effects of remote voting on the electoral process would need to be addressed before any such system could be responsibly deployed

Internet-based initial voter registration poses significant risk to the integrity of the voting process, and should not be implemented until an adequate authentication infrastructure is available and adopted. While information already in the domain of election officials may be updated remotely, given appropriate authentication protocols, initial registration conducted online cannot establish the identity of the registrant absent the transmission of smart card an existing database with which to verify it.

Online registration without the appropriate security infrastructure would be at high risk for automated fraud. The voter registration process is already one of the weakest links in our electoral process. The introduction of Internet-based registration with first addressing the considerable flaws in our current system would only serve to exacerbate the risks to which we are already exposed.

8. CONCLUSION AND SUGGESTION

This paper has highlighted the complexity of the deployment of smart cards operating under public key algorithms offers great advantages to guarantee both the voting anonymity and the voter's authentication. Since they are tamper-resistant, smart cards effectively protect personal keys of voters and the receipts generated after the internet voting. A new generation of smart cards, allow introducing in the card memory small applications, which support most of the needed cryptographic operations, maintaining in total secrecy the keys used for such operations. Although the small size of smart cards memory imposes certain limitations regarding the operations that can be carried out, adequate design and proper usage of existent tools permits to carry out complex and robust operations, which guarantee the global security of the system. There are currently no global standards for electronic ballots, and each system provides different solutions, which could be simplified if such a standard would be employed. With one common platform, it would be easier to concentrate efforts on developing and finding problems in internet voting systems. Malicious code checking program must be installed in the internet voting software. Work is needed to test the case where the internet voting system is run in parallel with an Electronic voting system, where voters can choose one of the systems to cast votes.

REFERENCES

[1] Alessandro Acquisti "*Receipt-Free Homomorphic Elections and Write-In Ballots"* – Technical Report 2004/105, International Association for Crypto Logic Research, May 2004.

[2] Cohen, J., and M. Fischer. "*A Robust And Verifiable Cryptographically Secure Election Scheme*." – Proceeding of the 26th IEEE Symposium on Foundations of Computer Science (October 1985):372-382.

[3] H. Nurmi, A. Salomaa, and L. Santean, "*Secret Ballot Elections In Computer Networks*," –Computers and Security 36(10), 2006.

[4] M.bellare, A. Boldyreva, and J. Staddon. Randomness "*Re-Use In Multi-Recipient Encryption Schemes"* – PKC 2003, Volume 2567, 2003.

[5] Neumann, Peter G. *"Security Criteria for Electronic Voting"* - 16th National Computer Security Conference (September 2007).

[6] Nurmi, H., et al. *"Secret Ballot Elections in Computer Networks"* - Computers & Security, Vol. 10(2008): 553-560.

[7] O. Baudron, P. Fouque, D. Pointcheval, J. Stern, and G. Poupard, *"Practical Multi-Candidate Election System"* – ACM 20-th Symposium on Principle of Distributed Computing, PODC'01, 2001.

[8] Peter Laud "*Symmetric Encryption In Automatic Analyses For Confidentiality Against Active Adversaries"* – IEEE Symposium on Security and Privacy.

[9] Saltman, Roy G. *"Computerized Voting"* – Chapter 5 In Advances In Computers, Vol. 32, Academic Press, 2009: 255-305.

August 2024

Vol-14 No:-8

@ IJITCE Publication